

Rogueware on an Explosive Trend...

By Sean-Paul Correll



In January 2009 *Inside the AV Lab* looked at rogue security software in 2008, a growing trend in fake security software. Since that time, we have experienced an explosion of fake security software infections emanating from all corners of the globe: rogueware threats have become a major threat, second only to the most commonly distributed malware – Trojans.

In Q1 of 2008, we had a little over 1,000 rogueware samples in our database; by the end of Q4 2008 we finished with 92,215. In Q1 2009 alone, we received 111,086 rogueware variants. Q2 brought in a staggering 374,204 new rogueware threats!

The growth of rogueware samples in 2008 prompted the lab to dedicate a team specifically to this type of threat. During our ongoing investigation, we discovered startling details about the financial background, as well as the distribution efforts behind this ever expanding threat landscape. In our most recent report entitled “*The Business of Rogueware*,”¹ we estimated that cybercriminals could be making up to \$34 million a month in these schemes.

The rogueware business model relies on the manufacturers, who are responsible for creating the fake software, and trustworthy affiliates to distribute them. The affiliates, mostly Eastern Europeans, make money on a per install basis (\$0.50-\$0.90 per install) as well as a 50-90 percent profit for completed sales.

In August 2008, a hacker, Neon, was able to infiltrate a leading rogueware manufacturer back-end website, revealing previously hidden financial data as well as the affiliate distribution system. In the break-in, NeoN revealed a six-day sales capture from a top-ranking affiliate: from August 23-28, the cybercriminal affiliate netted \$81,388 in profit.

Rogueware Distribution

Blackhat SEO is currently the most prevalent distribution method and one of the most dangerous because of user-implied trust in search results. A Forrester research study conducted in 2008 showed that 50 percent of Internet users trust content delivered by search engines.² The biggest blackhat SEO rogueware attack we observed targeted the Ford Motor Company and involved over 3 million search terms. Anyone searching for Ford news, car parts, or model numbers was greeted with malicious search results yielding more rogueware infectors.³

Social networks

Social networks are increasingly becoming a major target for rogueware distributors as well. Social network worms, such as the Koobface worm, have been known to target not only Facebook, but Twitter, MySpace, Hi5, and several other social networks. After worms, one of the biggest rogueware distribution effort in social media was an attack on the news aggregator, Digg.com. Cybercriminals were able to kill two birds with one stone by utilizing blackhat SEO and social engineering all in one shot. The attack consisted of a user-submitted story of a relevant and timely news subject and included a malicious comment. For example, a news submission referencing the death of the actor Heath Ledger was followed up with a malicious comment, which claimed to have a video of the actor in the shower. Upon viewing the site, a fake codec installation was prompted to distribute rogueware infectors onto the victim’s computer.⁴

Botnet distribution

Botnet monetization is not new by any means. Cybercriminals have been known to rent botnets out for malware distribution, spam, DDoS, and various other services, but for the first time we are starting to see rogueware pop up in botnet-infected endpoints. Massive outbreaks such as the Conficker worm used rogueware as a final measure to profit off the infected network. In April 2009, the Conficker infection network was estimated at 4 million,⁵ which means that the botnet owner could have profited \$3.6 million on the rogueware installations alone.

Conclusion

The rogueware business has grown to epic proportions and shows no sign of slowing. The software is getting more evasive by including technical solutions, such as “AV killer,” which are designed to disable legitimate security protection. In addition, cybercriminals are increasing their levels of sophistication by generating hundreds of thousands of new samples to escape antivirus detection for as long as possible. As a result of these new tactics and the success in which cybercriminals have had in profiting from this malware variant, we estimate that new Rogueware threats will grow to 637,322 samples by the end of Q3 2009.

About the author

Sean-Paul Correll is a threat researcher and security evangelist for Panda Security, specializing in malware surveillance and emerging threat discovery. He can be contacted at Sean-Paul.Correll@us.pandasecurity.com or <http://www.twitter.com/lithium>.

1 <http://bit.ly/plabs1>

2 <http://blogs.forrester.com/groundswell/2008/12/people-dont-tru.html>.

3 http://pandalabs.pandasecurity.com/archive/Targeted-Blackhat-SEO-Attack-against-Ford-Motor-Co_2E00_.aspx.

4 http://pandalabs.pandasecurity.com/archive/Have-you-ever-heard-the-term-_2200_Rickrolling_22003F00_-Malware-distributors-have_2E002E002E00_.aspx.

5 <http://mtc.sri.com/Conficker>.